Junos Pulse Mobile Security Dashboard

Benutzerhandbuch

Release
4.0

Juni 2012
R1

Copyright © 2012, Juniper Networks, Inc.

.

Junos® Pulse Mobile Security Dashboard

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089, USA
408-745-2000
www.juniper.net

Copyright © Juniper Networks, Inc.
Juni 2012

Juniper Networks, Junos, Steel-Belted Radius, NetScreen und ScreenOS sind in den USA und anderen Ländern eingetragene Marken von Juniper Networks, Inc. Das Juniper Networks-Logo, das Junos-Logo und JunosE sind Marken von Juniper Networks, Inc. Alle anderen Marken, Dienstleistungsmarken, eingetragenen Marken oder eingetragenen Dienstleistungsmarken sind Eigentum der jeweiligen Besitzer. Juniper Networks übernimmt keine Haftung für Fehler in diesem Dokument. Juniper Networks behält sich das Recht vor, diese Publikation ohne Ankündigung zu verändern, zu übertragen oder anderweitig zu überarbeiten. Von Juniper Networks hergestellte oder verkaufte Produkte oder Komponenten davon unterliegen möglicherweise einem oder mehreren der folgenden Patente (US-Patentnummern), die sich im Besitz von Juniper Networks befinden oder für Juniper Networks lizenziert sind: Patentnummern 5.473.599, 5.905.725, 5.909.440, 6.192.051, 6.333.650, 6.359.479, 6.406.312, 6.429.706, 6.459.579, 6.493.347, 6.538.518, 6.538.899, 6.552.918, 6.567.902, 6.578.186 und 6.590.785.
Copyright © 2011, Juniper Networks, Inc. Alle Rechte vorbehalten.

Inhalt

Zielgruppe v
Handbuchinhalt v
Typografische Konventionen v
Kontaktaufnahme mit dem technischen Support vi
Kapitel 1 **Einführung** 1
Funktionen des Junos Pulse Mobile Security Dashboard 1
Kapitel 2 **Arbeiten mit dem Mobile Security Dashboard** 3
Übersicht 3
Informationen und Befehle der Registerkarte "Startseite" 5
E-Mail-Validierung und Warnmeldung 5
Anti-Diebstahl-Schutz 6
Gerät sperren/Zugangscode zurücksetzen 6
Gerät entsperren/Zugangscode zurücksetzen 7
Gerät vollständig löschen 8
Scream 9
Gerät suchen 9
Geräteüberwachung 10
Antivirenaktivität 11
Sichern Ihrer Daten 11
Benutzerdefinierte Schaltfläche 12
Informationen und Konfiguration des Links für Einstellungen 12
Kontenverwaltung 12
Handset-Management 12
Informationen und Konfiguration der Registerkarte "Berichte" 14
Verlauf 15
Informationen und Konfiguration der Registerkarte "Warnungseinrichtung" 15
Informationen und Konfiguration der Registerkarte "Support/Hilfe" 16
Kapitel 3 **Junos Pulse FAQ** 17
Junos Pulse FAQs 17

:

Copyright © 2012, Juniper Networks, Inc.

Über dieses Benutzerhandbuch

In diesem Benutzerhandbuch wird beschrieben, wie Sie das Junos® Pulse Mobile Security Dashboard verwenden, um registrierte Mobilgeräte zu verwalten und Funktionen wie bspw. das vollständige Löschen und die Remote-Sperre zu aktivieren, falls ein Gerät verloren gegangen ist oder gestolten wurde.

Informativer Hinweis: Informationen zur Installation und Konfiguration von Junos Pulse auf einzelnen Mobilgeräten finden Sie für diesen Gerätetyp in der Junos Pulse-Dokumentation.

Zielgruppe

Dieses Handbuch ist für Benutzer gedacht, die Steuerelemente für Gerätebenutzer konfigurieren möchten, um Sicherheitsfunktionen und Zugriffssteuerungsfunktionen bereitzustellen.

Handbuchinhalt

Dieses Handbuch ist in folgende Kapitel gegliedert:

- Kapitel 1, “Einführung” auf Seite 1
- Kapitel 2, “Arbeiten mit dem Mobile Security Dashboard” auf Seite 3
- Kapitel 3, “Junos Pulse FAQ” auf Seite 17

Typografische Konventionen

Tabelle 1 erläutert die in diesem Benutzerhandbuch verwendeten Konventionen.

Tabelle 1: Typografische Konventionen

Konvention	Beschreibung	Beispiele
Fette Schriftart	Zeigt Schaltflächen, Feldnamen, Dialogfeldnamen und andere Elemente der Benutzeroberfläche an.	Verwenden Sie zum Planen einer Konferenz die Registerkarten Scheduling (Planung) und Appointment (Termin).
Plain Sans Serif	Stellt Folgendes dar: • URLs, Dateinamen und Verzeichnisse	Beispiel: • URL: Laden Sie die JRE-Anwendung unter http://java.sun.com/j2se/ herunter.
Kursiv	Stellt Folgendes dar: • Im Text definierte Begriffe • Variable Elemente • Buchnamen	Beispiele: • Variables Element: Verwenden Sie die Einstellungen auf der Seite Benutzer > Rollen > Rolle auswählen, um Rollen zu konfigurieren.

Copyright © 2012, Juniper Networks, Inc.

Kontaktaufnahme mit dem technischen Support

Sie können den technischen Produktsupport über das Juniper Networks Technical Assistance Center (JTAC) anfordern. Wenn Sie Kunde mit einem gültigen J-Care- oder JNASC-Supportvertrag sind oder Anspruch auf Garantieleistungen haben und technischen Support benötigen, können Sie online auf unsere Tools und Ressourcen zugreifen oder über das JTAC einen Supportfall öffnen.

- JTAC-Richtlinien: Ausführliche Informationen zu den JTAC-Verfahren und -Richtlinien finden Sie im JTAC Benutzerhandbuch unter http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Produktgarantien: Informationen zur Produktgarantie finden Sie unter http://www.juniper.net/support/warranty/.
- JTAC-Geschäftszeiten: Die Mitarbeiter in den JTAC-Centern sind rund um die Uhr und an allen Tagen der Woche für Sie da.

Copyright © 2012, Juniper Networks, Inc.

Kapitel 1

Einführung

Das Junos® Pulse Mobile Security Dashboard sammelt Daten zugewiesener Mobilgeräte und lädt diese Daten in das Dashboard hoch, auf das mit einem Benutzernamen und einem Kennwort über das Internet zugegriffen werden kann. Über das Junos Pulse Mobile Security Dashboard können Sie registrierte Mobilgeräte verwalten und Funktionen wie bspw. das vollständige Löschen aktivieren, falls ein Gerät verloren gegangen ist oder gestohlen wurde. Sie können für verdächtige Nachrichten, die auf dem Gerät empfangen oder vom Gerät gesendet wurden, auch E-Mail-Warnmeldungen konfigurieren. In diesem Fall werden Nachrichten, die benutzerdefinierte Schlüsselwörter enthalten (z. B. Drogen, Alkohol oder Nachrichten, die von bestimmten Adressen stammen oder an bestimmte Adressen geleitet werden), automatisch per E-Mail an Sie gesendet.

Funktionen des Junos Pulse Mobile Security Dashboard

Das Junos Pulse Mobile Security Dashboard stellt für registrierte Mobilgeräte Steuerung und Sicherheit bereit.

In den Steuerungsfunktionen ist Folgendes enthalten:

- Überwachen der Aktivität auf dem Gerät.
- Zeigen Sie Bilder an, die mit der Gerätekamera aufgenommen wurden oder in einer Textnachricht oder einer E-Mail gesendet oder empfangen wurden.
- Zeigen Sie den Inhalt aller Text- und E-Mail-Nachrichten an.
- Empfangen Sie automatisch Warnmeldungen, wenn in gesendeten oder empfangenen Nachrichten Schlüsselwörter enthalten sind.
- Führen Sie alle auf dem Gerät installierten Anwendungen und Software auf.
- Zeigen Sie den Standort des Geräts auf einer Online-Karte an.
- Geben Sie einen Alarmton auf dem Gerät aus.
- Verwenden Sie GPS, um ein verloren gegangenes oder gestohlenes Gerät aufzufinden. (Die GPS-Funktionalität steht auf den Verizon BlackBerry Curve- und Storm 1-Smartphones eventuell nicht zur Verfügung. Wenn Sie GPS-Längen- und Breitenkoordinaten von 0,0 haben, kann es sein, dass diese Funktionalität vom Dienstanbieter blockiert wurde oder dass das Gerät sich außerhalb des Bereichs eines Satelliten befindet.)

Copyright © 2012, Juniper Networks, Inc.

In den Sicherheitsfunktionen ist Folgendes enthalten:

- Antivirus: Diese Funktion bietet einen Schutz in Echtzeit gegen Malware-Bedrohungen, indem Geräte automatisch gescannt werden, um sicherzustellen, dass keine Dateien mit Malware infiziert sind. Mit der Scanfunktion auf Abruf können Sie ausgewählte Dateien und Ordner scannen, um sicherzustellen, dass das Gerät und die Speicherkarte virenfrei und geschützt sind. Die Funktion zur automatischen Aktualisierung stellt sicher, dass auf dem Gerät die neuesten Antivirussignaturen vorhanden sind.
- Sicherung/Wiederherstellung: Mit dieser Funktion können Sie Kontakt- und Kalenderinformationen sichern.
- Firewall: Mit den Firewall-Sicherheitsfunktionen können Sie anhand von Regellisten, die den Datenverkehr basierend auf der Portnummer und IP-Adressen steuern, den Datenverkehr von und zu Ihrem Gerät blockieren oder zulassen.
- Anti-Diebstahl-Schutz: In diesen Funktionen sind Remote-Befehle enthalten, die Sie an das Gerät senden können, wenn es verloren gegangen ist oder gestohlen wurde. Folgende Befehle sind enthalten: Gerät sperren, Gerät vollständig löschen, Gerät finden und Gerät sichern.

Copyright © 2012, Juniper Networks, Inc.

Kapitel 2

Arbeiten mit dem Mobile Security Dashboard

In diesem Kapitel wird der Zugriff auf und das Arbeiten mit dem Junos Pulse Mobile Security Dashboard beschrieben, um Überwachungs- und Sicherheitsfunktionen für registrierte Geräte zu konfigurieren.

Übersicht

Informativer Hinweis: Bevor Sie sich am Mobile Security Dashboard anmelden können, müssen Sie Junos Pulse auf Ihrem Mobilgerät installieren und registrieren. Informationen zur Installation von Junos Pulse, zur Registrierung und zu den Details der Konfiguration für Ihren Gerätetyp finden Sie im Junos Pulse Benutzerhandbuch (Android, BlackBerry, iOS, Windows Mobile, Symbian).

Wenn die Junos Pulse-Anwendung auf dem Gerät installiert ist und Sie während der Installation und Registrierung des Geräts eine E-Mail-Adresse und ein Kennwort eingerichtet haben, können Sie diese E-Mail-Adresse und dieses Kennwort für die Anmeldung am Mobile Security Dashboard verwenden. Der Zugriff auf das Dashboard erfolgt über die URL, die Sie von Ihrem Administrator oder Dienstanbieter erhalten haben. (Siehe Abbildung 1 auf Seite 4).

Sie können sich auch mit Ihrer Telefonnummer und Ihrem Kennwort anmelden. Die Telefonnummer, die Sie eingeben, muss identisch sein mit der Telefonnummer, die Sie bei der Registrierung des Geräts eingegeben haben. Sie können keine Zeichen verwenden, die bei der Registrierung nicht als Teil der Telefonnummer verwendet wurden.

Informativer Hinweis: Wenn Sie sich mit einer Telefonnummer anmelden, können Sie nur diese Geräteinformationen im Dashboard anzeigen. Wenn Sie jedoch mehrere registrierte Geräte unter einem Benutzernamen haben, können Sie alle Geräte anzeigen, wenn Sie sich mit diesem Benutzernamen anmelden.

Zurücksetzen des Kennworts

Wenn Sie Ihr Anmeldekennwort für das Dashboard vergessen haben, können Sie es zurücksetzen, indem Sie auf der Startseite auf den Link **Kennwort vergessen?** klicken. Wenn Sie auf diesen Link klicken, gelangen Sie zu einem neuen Fenster, von wo aus Sie Folgendes tun müssen:

1. Geben Sie Ihre **E-Mail-Adresse** ein.
2. Geben Sie die letzten **vier Ziffern** Ihrer Telefonnummer ein.
3. Klicken Sie auf **Kennwort zurücksetzen**.

Copyright © 2012, Juniper Networks, Inc.

Wenn Sie auf die Schaltfläche "Kennwort zurücksetzen" klicken, wird ein neues Kennwort für Sie erstellt und per E-Mail an Sie gesendet. Verwenden Sie dieses Kennwort, wenn Sie sich das nächste Mal anmelden. Nach einer erfolgreichen Anmeldung können Sie Ihr Kennwort zu einem anderen, das Sie vorziehen, ändern. (Siehe Kontenverwaltung auf Seite 12).

Abbildung 1: Anmeldefenster von Mobile Security Dashboard

Wenn Sie sich angemeldet haben, wird die Registerkarte "Startseite" angezeigt. (Siehe Abbildung 2 auf Seite 5). Neben der Registerkarte "Startseite" finden Sie Registerkarten und Links für jeden Funktionsbereich des Dashboard. Diese Registerkarten und Links lauten wie folgt:

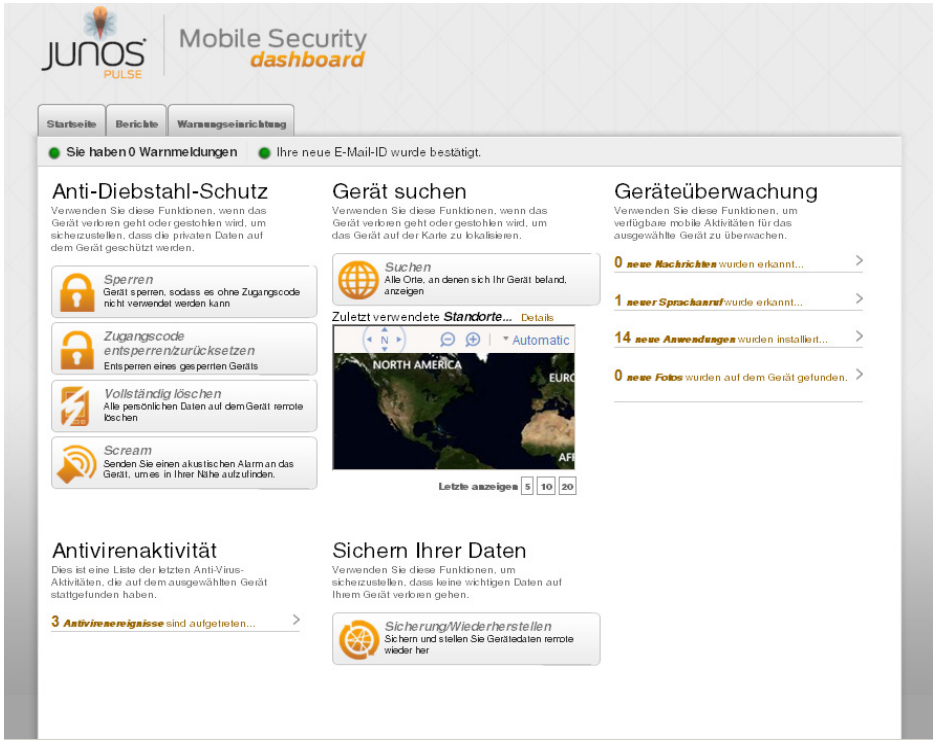
Informativer Hinweis: Junos Pulse kann mit allen verfügbaren Funktionen oder mit Unterfunktionen, die auf den Anforderungen des Benutzers basieren, bereitgestellt werden. Möglicherweise sind auf Ihrem Gerät nicht alle hier beschriebenen Funktionen auf Ihrem Dashboard sichtbar.

- Startseite: Wenn Sie das Dashboard konfiguriert haben, werden in der Registerkarte "Startseite" alle benötigten Informationen und Befehle auf einen Blick bereitgestellt. Links zu Diebstahlsicherungsbefehlen, protokollierten Nachrichten und Anrufen, aufgefundenen Viren, Ereignissen, installierten Anwendungen und Fotos werden bereitgestellt. Auch die letzten GPS-Standorte und die Möglichkeit, die Daten des ausgewählten Geräts zu sichern und wiederherzustellen werden bereitgestellt.
- Berichte: Konfigurieren Sie Berichtsfilter, um basierend auf dem Datum nach bestimmten Absendern oder Schlüsselwörtern in einem Bereich von Nachrichten zu suchen.
- Warnungseinrichtung: Konfigurieren Sie Parameter, um Warnungen auszulösen. (Wenn Sie auf die Warnungsmeldung klicken, wenn sie verfügbar ist, finden Sie auch den Warnstatus und können Warnungen konfigurieren, wie sie unter den Registerkarten auf der Registerkarte "Startseite" angezeigt werden.)
- Einstellungen: Konfigurieren Sie über den Link "Einstellungen", der immer oben im Dashboardfenster zur Verfügung steht, unterschiedliche Benutzerkonten und Geräte, die Sie überwachen möchten.

Informativer Hinweis: Beachten Sie, dass Warnungseinstellungen nicht für iOS-Geräte zur Verfügung stehen.

Copyright © 2012, Juniper Networks, Inc.

Abbildung 2: Registerkarte "Startseite"


JUNOS PULSE
Mobile Security dashboard
Startseite
Berichte
Warnungseinrichtung
Sie haben 0 Warnmeldungen
Ihre neue E-Mail-ID wurde bestätigt.
Anti-Diebstahl-Schutz
Verwenden Sie diese Funktionen, wenn das Gerät verloren geht oder gestohlen wird, um sicherzustellen, dass die privaten Daten auf dem Gerät geschützt werden.
Sperren
Gerät sperren, sodass es ohne Zugangscode nicht verwendet werden kann
Zugangscode entsperren/zurücksetzen
Entsperren eines gesperrten Geräts
Vollständig löschen
Alle persönlichen Daten auf dem Gerät remote löschen
Scream
Senden Sie einen akustischen Alarm an das Gerät, um es in Ihrer Nähe aufzufinden.
Gerät suchen
Verwenden Sie diese Funktionen, wenn das Gerät verloren geht oder gestohlen wird, um das Gerät auf der Karte zu lokalisieren.
Suchen
Alle Orte, an denen sich Ihr Gerät befand, anzeigen
Zuletzt verwendete Standorte... Details
Automatic
NORTH AMERICA
Letzte anzeigen 5 10 20
Geräteüberwachung
Verwenden Sie diese Funktionen, um verfügbare mobile Aktivitäten für das ausgewählte Gerät zu überwachen.
0 neue Nachrichten wurden erkannt...
1 neuer Sprachanruf wurde erkannt...
14 neue Anwendungen wurden installiert...
0 neue Fotos wurden auf dem Gerät gefunden.
Antivirenaktivität
Dies ist eine Liste der letzten Anti-Virus-Aktivitäten, die auf dem ausgewählten Gerät stattgefunden haben.
3 Antivirenereignisse sind aufgetreten...
Sichern Ihrer Daten
Verwenden Sie diese Funktionen, um sicherzustellen, dass keine wichtigen Daten auf Ihrem Gerät verloren gehen.
Sicherung/Wiederherstellen
Sichern und stellen Sie Gerätedaten remote wieder her

Informationen und Befehle der Registerkarte "Startseite"

Auf der Registerkarte "Startseite" werden auf einen Blick alle Informationen und Befehle für das ausgewählte Gerät bereitgestellt. Wählen Sie ein Gerät über das Pulldownmenü oben rechts im Dashboardfenster aus. Auf der Registerkarte "Startseite" wird ggf. Folgendes bereitgestellt:

E-Mail-Validierung und Warnmeldung

Im Benachrichtigungsabschnitt werden auf der Registerkarte "Startseite" unter den Registerkarten Informationen für das ausgewählte Gerät angezeigt. Die hier bereitgestellten Informationen können Folgendes umfassen:

- Warnmeldungen: Wenn für ein Gerät Warnungen vorhanden sind, werden diese Informationen hier veröffentlicht. Siehe Informationen und Konfiguration der Registerkarte "Warnungseinrichtung" auf Seite 15 für weitere Informationen.
- Email validation status (Status der E-Mail-Validierung): Wenn Benutzer ein Gerät erfolgreich registriert haben, empfangen Sie nach der ersten Anmeldung am Dashboard eine E-Mail, in der sie aufgefordert werden, ihre E-Mail-Adresse zu validieren. In dieser E-Mail ist ein Link enthalten, auf den die Benutzer klicken müssen, um ihre E-Mail-Adresse zu validieren. Nachdem sie auf den Link geklickt haben, wird eine Webseitenbenachrichtigung angezeigt, um sie zu informieren, dass die E-Mail-Adresse validiert wurde.

Informativer Hinweis: Eine Anforderung für eine E-Mail-Validierung wird auch gesendet, wenn auf dem Dashboard eine E-Mail-Adresse bearbeitet wird. (Siehe Kontenverwaltung auf Seite 12).

Copyright © 2012, Juniper Networks, Inc.

Anti-Diebstahl-Schutz

Klicken Sie auf die verfügbaren Befehlsschaltflächen "Anti-Diebstahl-Schutz", um den entsprechenden Befehl zu senden. Wenn Sie auf eine Befehlsschaltfläche klicken, wird ein Popupfenster angezeigt, in dem Sie aufgefordert werden, den ausgewählten Befehl zu bestätigen, bevor er gesendet wird. In manchen Fällen müssen Sie auch zusätzliche Informationen eingeben.

Gerät sperren/Zugangscode zurücksetzen

Wenn Sie für das ausgewählte Gerät auf diese Schaltfläche klicken, wird ein Popupfenster angezeigt. Von diesem Fenster aus können Sie einen Befehl senden, über den das Gerät gesperrt wird, wenn es verloren gegangen ist oder gestohlen wurde oder wenn Sie die Verwendung des Geräts aus irgendeinem anderen Grund beenden möchten.

Bei Android- und BlackBerry-Geräten stellt das Popupfenster einen zufällig erzeugten Sperrzugangscode bereit, der zusammen mit dem Sperrbefehl an das Gerät gesendet werden kann (siehe Abbildung 3 auf Seite 7). Sie können diesen Sperrzugangscode vor dem Senden des Befehls bearbeiten. Wenn Sie einen neuen Zugangscode senden, können Sie über das Kontrollkästchen auswählen, dass der Zugangscode per E-Mail an den Gerätebenutzer gesendet werden soll. Der Befehl für den Sperrzugangscode funktioniert auf folgende Weise:

- Auf Android-Geräten:
  - Wenn der Geräteadministrator aktiviert ist und für das Gerät schon ein Kennwort konfiguriert wurde:
    - Wenn ein Sperrbefehl mit einem neuen Kennwort gesendet wurde, wird das Gerät mit dem bestehenden Kennwort gesperrt. Das neue Kennwort vom Server wird nicht verwendet.
    - Wenn ein Sperrbefehl mit einem leeren Kennwort gesendet wird, wird das Gerät mit dem bestehenden Kennwort gesperrt. Das Kennwort vom Server wird nicht verwendet.
  - Wenn der Geräteadministrator aktiviert ist und für das Gerät noch kein Kennwort konfiguriert wurde:
    - Wenn ein Sperrbefehl mit einem neuen Kennwort gesendet wurde, wird das Gerät mit diesem neuen Kennwort gesperrt.
    - Wenn ein Sperrbefehl mit einem leeren Kennwort gesendet wird, wird das Gerät NICHT gesperrt.
  - Wenn der Geräteadministrator deaktiviert ist und das Gerät automatisch registriert wird:
    - Wenn ein Sperrbefehl mit einem neuen Kennwort gesendet wurde, wird das Gerät mit diesem neuen Kennwort gesperrt. (Unabhängig vom auf dem Gerät konfigurierten Kennwort.)
    - Wenn ein Sperrbefehl mit einem leeren Kennwort gesendet wird, wird das Gerät NICHT gesperrt.
  - Wenn der Geräteadministrator deaktiviert ist und das Gerät manuell registriert wird:
    - Wenn ein Sperrbefehl mit einem neuen Kennwort gesendet wurde, wird das Gerät mit diesem neuen Kennwort gesperrt. (Unabhängig vom auf dem Gerät konfigurierten Kennwort.)

Copyright © 2012, Juniper Networks, Inc.

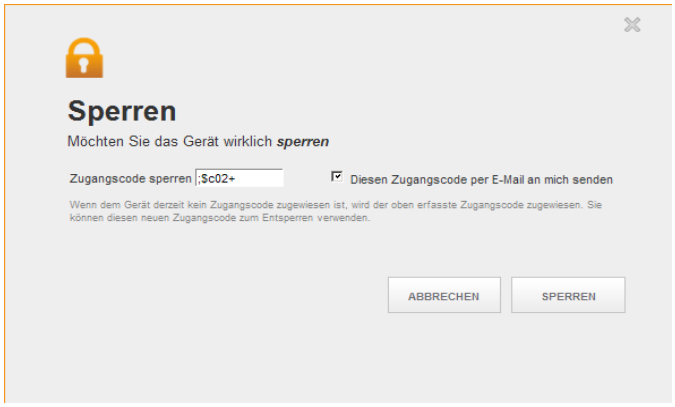
  - Wenn ein Sperrbefehl mit einem leeren Kennwort gesendet wird, wird das Gerät NICHT gesperrt.

- Auf BlackBerry-Geräten:
  - Wenn das Gerät automatisch registriert wurde:
    - Wenn ein Sperrbefehl mit einem neuen Kennwort gesendet wurde, wird das Gerät mit diesem neuen Kennwort gesperrt.
    - Wenn ein Sperrbefehl mit einem leeren Kennwort gesendet wird, wird das Gerät mit dem auf dem Gerät erstellten zufälligen Kennwort gesperrt. Dieses Kennwort wird nicht per E-Mail gesendet.
  - Wenn das Gerät manuell registriert wurde:
    - Wenn ein Sperrbefehl mit einem neuen Kennwort gesendet wurde, wird das Gerät mit diesem neuen Kennwort gesperrt.
    - Wenn ein Sperrbefehl mit einem leeren Kennwort gesendet wird, wird das Gerät mit dem während der Registrierung verwendeten Kennwort gesperrt. Dieses Kennwort wird nicht per E-Mail gesendet.

Informativer Hinweis: Auf allen anderen Geräten muss ein Entsperrbefehl gesendet werden, um das Gerät zu entsperren, wenn ein Sperrbefehl gesendet wurde.

Klicken Sie auf die Schaltfläche **Sperren**, um den Sperrbefehl zu senden, oder klicken Sie auf **Abbrechen**, um keinen Befehl zu senden.

Abbildung 3: Popupfenster Sperren


Sperren
Möchten Sie das Gerät wirklich sperren
Zugangscode sperren ;$c02+
Diesen Zugangscode per E-Mail an mich senden
Wenn dem Gerät derzeit kein Zugangscode zugewiesen ist, wird der oben erfasste Zugangscode zugewiesen. Sie können diesen neuen Zugangscode zum Entsperren verwenden.
ABBRECHEN
SPERREN

Gerät entsperren/Zugangscode zurücksetzen

Wenn Sie für das ausgewählte Gerät auf diese Schaltfläche klicken, wird ein Popupfenster angezeigt. Von diesem Fenster aus können Sie einen Befehl senden, mit dem das Gerät entsperrt wird oder der Zugangscode auf iOS-Geräten gelöscht wird, sodass Benutzer ein neues Kennwort eingeben können, um das Gerät zu entsperren.

Bei Android- und BlackBerry-Geräten stellt das Popupfenster einen zufällig erzeugten Zugangscode bereit, der zusammen mit dem Entsperrbefehl an das Gerät gesendet werden kann (siehe Abbildung 3 auf Seite 7). Sie können diesen Entsperrzugangscode vor dem Senden des Befehls bearbeiten. Wenn Sie einen neuen Zugangscode senden, können Sie über das Kontrollkästchen auswählen, dass der Zugangscode per E-Mail an den Gerätebenutzer gesendet werden soll. Der Benutzer muss den neuen Zugangscode eingeben, um das Gerät zu entsperren.

Copyright © 2012, Juniper Networks, Inc.

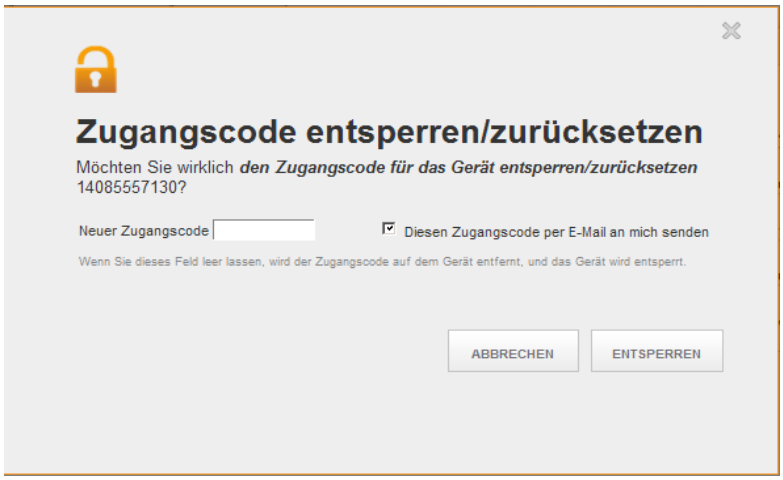
Informativer Hinweis: Wenn der Geräteadministrator bei Android-Geräten aktiviert ist und auf dem Gerät ein Zugangscode definiert wurde, ersetzt der neue Zugangscode den bestehenden Zugangscode nur, wenn die Zugangscoderichtlinie des Geräts erfüllt wird. Ein leerer Zugangscode entsperrt das Gerät nur, wenn das Gerät einen leeren Zugangscode zulässt und die Verschlüsselung nicht aktiviert ist.

Informationen zum Sperren eines Geräts basierend auf verschiedenen Bedingungen finden Sie im vorigen Abschnitt **Gerät sperren/Zugangscode zurücksetzen** auf Seite 6.

Informativer Hinweis: Bei allen anderen Geräten entsperrt ein Entsperrbefehl das Gerät. Das Feld "Zugangscode" wird nicht unterstützt.

Klicken Sie auf die Schaltfläche **Entsperren**, um den Entsperrbefehl zu senden, oder klicken Sie auf **Abbrechen**, um keinen Befehl zu senden.

Abbildung 4: Popupfenster "Unlock Device" (Gerät entsperren)


Zugangscode entsperren/zurücksetzen
Möchten Sie wirklich den Zugangscode für das Gerät entsperren/zurücksetzen 14085557130?
Neuer Zugangscode
Diesen Zugangscode per E-Mail an mich senden
Wenn Sie dieses Feld leer lassen, wird der Zugangscode auf dem Gerät entfernt, und das Gerät wird entsperrt.
ABBRECHEN
ENTSPERREN

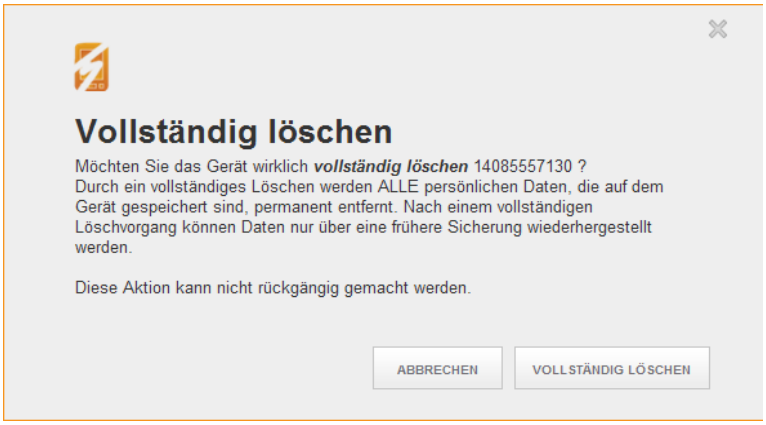
Gerät vollständig löschen

Wenn Sie für das ausgewählte Gerät auf diese Schaltfläche klicken, wird ein Popupfenster angezeigt. Von diesem Fenster aus können Sie einen Befehl senden, mit dem das Gerät gelöscht wird. Unterschiedliche Geräte unterstützen unterschiedliche Löschmöglichkeiten. In manchen Fällen wird das Gerät durch einen Löschbefehl auf die Werkseinstellungen zurückgesetzt. In anderen Fällen entfernt ein Löschbefehl nur persönliche Daten vom Gerät, wie z. B. Kontakte, Kalenderereignisse, Hinweise, Anrufverlauf, Nachrichtenordner und alle Daten auf der SD-Karte. Es ist nicht möglich zu konfigurieren, wie das Löschen auf den einzelnen Geräten funktioniert. Weitere Informationen zum Löschbefehl auf diesem Gerätetyp finden Sie in der Gerätedokumentation des Junos Pulse Benutzerhandbuchs.

Klicken Sie auf die Schaltfläche **Vollständig löschen**, um den Befehl zum vollständigen Löschen des Geräts zu senden, oder klicken Sie auf **Abbrechen**, um keinen Befehl zu senden (siehe Abbildung 5 auf Seite 9). Wenn Sie auf "Vollständig löschen" klicken, wird ein weiteres Popupfenster angezeigt, in dem Sie aufgefordert werden, das **vollständige Löschen** zu bestätigen.

Copyright © 2012, Juniper Networks, Inc.

Abbildung 5: Popupfenster "Gerät vollständig löschen"


Vollständig löschen
Möchten Sie das Gerät wirklich vollständig löschen 14085557130 ?
Durch ein vollständiges Löschen werden ALLE persönlichen Daten, die auf dem Gerät gespeichert sind, permanent entfernt. Nach einem vollständigen Löschvorgang können Daten nur über eine frühere Sicherung wiederhergestellt werden.
Diese Aktion kann nicht rückgängig gemacht werden.
ABBRECHEN
VOLLSTÄNDIG LÖSCHEN

Scream

Wenn Sie für das ausgewählte Gerät auf diese Schaltfläche klicken, wird ein Popupfenster angezeigt. Von diesem Fenster aus können Sie einen Scream-Befehl an das Gerät senden, mit dem der Benutzer das verlegte Gerät akustisch orten kann, wenn es sich in Hörweite befindet. Dies funktioniert auch dann, wenn die Lautsprecher und der Rufton stumm geschaltet sind.

Klicken Sie vom Popupfenster "Scream" auf **An**, um einen Scream-Befehl zu senden. Klicken Sie auf **Aus**, um einen Befehl zum Ausschalten von Scream zu senden. Klicken Sie auf **Abbrechen**, um keinen Befehl zu senden (siehe Abbildung 6 auf Seite 9).

Abbildung 6: Popupfenster "Scream"

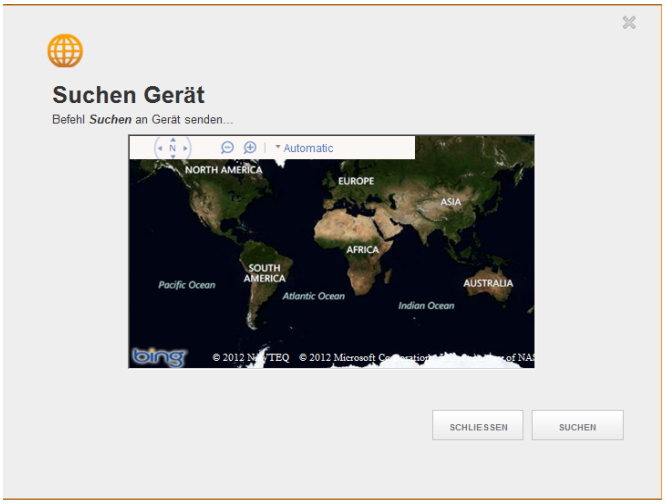
Gerät suchen

Klicken Sie auf der Registerkarte "Startseite" auf **Suchen**, um das Popupfenster "Suchen Gerät" anzuzeigen. Von diesem Fenster aus können Sie einen Befehl senden, um den GPS-Standort des Geräts zu bestimmen. Das Ergebnis wird im Popupfenster "Suchen Gerät" und auf der Registerkarte "Startseite" angezeigt.

Klicken Sie im Popupfenster "Suchen Gerät" auf **Suchen**, um einen Suchbefehl zu senden. Klicken Sie auf **Schließen**, um keinen Befehl zu senden (siehe Abbildung 7 auf Seite 10).

Copyright © 2012, Juniper Networks, Inc.

Abbildung 7: Popupfenster "Suchen Gerät"



Informativer Hinweis: GPS wird auf dem iPod Touch und auf iOS-Geräten, die über keinen Mobildienst verfügen, nicht unterstützt.

Informativer Hinweis: Es gibt keine für IOS-Geräte verfügbaren Befehle, die über kein entsprechendes APNS-Zertifikat verfügen. Wenn kein APNS-Zertifikat vorhanden ist, ist der GPS-Standort die einzige verfügbare Funktion.

Geräteüberwachung

Wenn es für eine verfügbare Überwachungskategorie für das ausgewählte Gerät Ereignisse gibt, wird die Anzahl der Ereignisse für jede Kategorie unter "Geräteüberwachung" als klickbarer Link angezeigt.

Wenn Sie auf einen dieser Ereignislinks klicken, wird ein Fenster angezeigt, in dem die Ereignisse für diese Kategorie angezeigt werden. In jedem einzelnen Ereignistypfenster können Sie Ereignisse verwalten, indem Sie das Kontrollkästchen neben dem Element, das Sie entfernen möchten, aktivieren und auf die Schaltfläche **Löschen** klicken. Sie können auch das Kontrollkästchen oben in der Spalte mit den Kontrollkästchen aktivieren und auf die Schaltfläche **Löschen** klicken, um alle Ereignisse in dieser Ereigniskategorie zu löschen.

Klicken Sie auf die Schaltfläche **Aktualisieren**, um das Gerät abzufragen. Dadurch lädt das Gerät neue Ereignisse hoch, die noch nicht an das Dashboard gesendet wurden.

Die verfügbaren Ereignisse können einen oder mehrere der folgenden Punkte umfassen:

- **Neue Nachrichten**: Zeigen Sie auf dem Gerät empfangene Nachrichten (Sprachanrufe, E-Mail, Text) an.
- **Neue Sprachanrufe**: Zeigen Sie auf dem Gerät empfangene Sprachanrufe an.
- **Neue Anwendungen**: Zeigen Sie neue Anwendungen an, die auf dem Gerät installiert wurden. Sie können eine Anwendung remote deinstallieren, indem Sie auf das Kontrollkästchen neben der Anwendung klicken und auf die Schaltfläche **Uninstall specific application** (Bestimmte Anwendung deinstallieren) auf dem Handset klicken.
- **Neue Fotos**: Zeigen Sie neue Fotos an, die auf dem Gerät gespeichert sind. Im Fotoereignisfenster werden 20 Fotos pro Fenster angezeigt.

Informativer Hinweis: Neue Anwendungen ist der einzige verfügbare Ereignistyp, der derzeit für iOS-Geräte verfügbar ist.

Copyright © 2012, Juniper Networks, Inc.

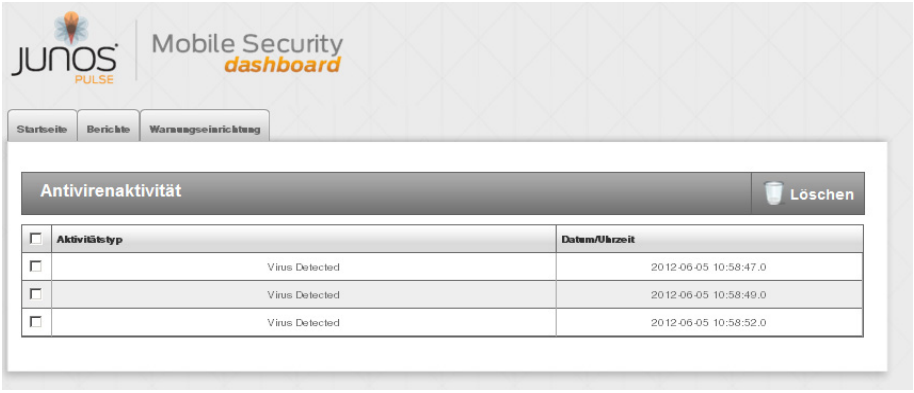
Antivirenaktivität

Wenn für das ausgewählte Gerät Antivirenereignisse vorhanden sind, werden diese Ereignisse als klickbare Links im Abschnitt "Antivirenaktivität" der Registerkarte "Startseite" angezeigt (siehe Abbildung 2 auf Seite 5). Wenn Sie auf der Registerkarte "Startseite" auf den Link **<#> Anti_Virus events occurred** (Antivirenereignisse aufgetreten) klicken, wird das Fenster mit der Ereignisliste "Antivirenaktivität" angezeigt, von wo aus Sie weitere Einzelheiten anzeigen und Antivirenereignisse verwalten können (siehe Abbildung 8 auf Seite 11).

Sie können Antivirenereignisse verwalten, indem Sie auf das Kontrollkästchen neben dem Element, das Sie entfernen möchten und auf die Schaltfläche **Löschen** klicken. Sie können auch das Kontrollkästchen oben in der Spalte mit den Kontrollkästchen aktivieren und auf die Schaltfläche **Löschen** klicken, um alle Antivirenereignisse zu löschen.

Klicken Sie auf die Schaltfläche **Aktualisieren**, um das Gerät abzufragen. Dadurch lädt das Gerät neue Ereignisse hoch, die noch nicht an das Dashboard gesendet wurden.

Abbildung 8: Fenster für Antiviren-Aktivitätsereignisse

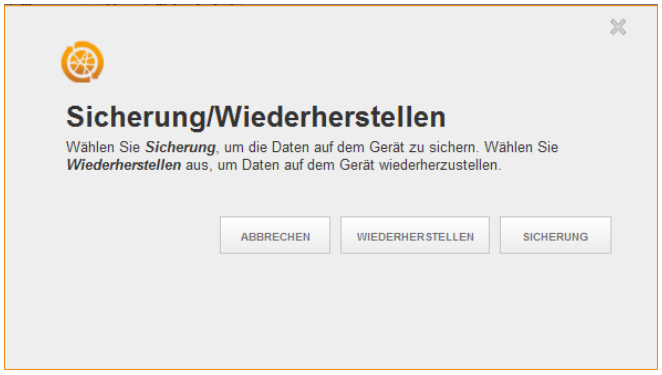


Sichern Ihrer Daten

Wenn Sie für das ausgewählte Gerät von der Registerkarte "Startseite" aus auf diese Schaltfläche klicken, wird ein Popupfenster angezeigt. Von diesem Fenster aus können Sie Daten auf dem ausgewählten Gerät remote sichern oder wiederherstellen. Über einen Wiederherstellungsbefehl wird eine Kopie der Kontakt- und Kalenderinformationen des Geräts erstellt. Dies ist hilfreich, wenn ein Gerät verloren gegangen ist oder gestohlen wurde.

Klicken Sie im Popupfenster "Sichern Ihrer Daten" auf die Schaltfläche **Sicherung**, um einen Sicherungsbefehl zu senden. Klicken Sie auf die Schaltfläche **Wiederherstellen**, um einen Wiederherstellungsbefehl zu senden. Klicken Sie auf die Schaltfläche **Abbrechen**, um keinen Befehl zu senden (siehe Abbildung 9 auf Seite 11).

Abbildung 9: Popupfenster "Sichern Ihrer Daten"


Sicherung/Wiederherstellen
Wählen Sie Sicherung, um die Daten auf dem Gerät zu sichern. Wählen Sie Wiederherstellen aus, um Daten auf dem Gerät wiederherzustellen.
ABBRECHEN
WIEDERHERSTELLEN
SICHERUNG

Copyright © 2012, Juniper Networks, Inc.

Benutzerdefinierte Schaltfläche

Wenn Ihr Geräteadministrator oder Dienstanbieter diese Funktion sichtbar gemacht hat, wird eine weitere benutzerdefinierte Schaltfläche auf der Registerkarte "Startseite" angezeigt. Wenn Sie auf diese Schaltfläche klicken, gelangen Sie über eine benutzerangepasste URL zu einer von Ihrem Dienstanbieter eingerichteten Webseite. Auf dieser Seite wird Ihnen ggf. angeboten, weitere Funktionen zu kaufen, oder zusätzliche Informationen werden bereitgestellt. Dies unterscheidet sich je nach Dienstanbieter.

Informationen und Konfiguration des Links für Einstellungen

Über den Link "Einstellungen" oben im Dashboardfenster können Sie die Kontenverwaltung und das Handset-Management konfigurieren. (Siehe Abbildung 10 auf Seite 14).

Kontenverwaltung

Sie können E-Mail-Adressen entfernen, bearbeiten oder einem Gerätekonto eine neue E-Mail-Adresse hinzufügen.

So fügen Sie eine E-Mail-Adresse und das entsprechende Kennwort hinzu:

1. Klicken Sie auf den Link **Einstellungen**.
2. Wählen Sie aus dem Pulldownmenü **Telefon zum Anzeigen auswählen** oben rechts das Gerät aus, das Sie verwalten möchten.
3. Zum Hinzufügen einer neuen E-Mail-Adresse für die Handset-Kontenverwaltung geben Sie in das Bearbeitungsfeld **Benutzername (E-Mail)** die E-Mail-Adresse ein.
4. Geben Sie das neue Kennwort in das Bearbeitungsfeld **Kennwort** ein.
5. Klicken Sie auf die Schaltfläche **Benutzer hinzufügen**.

Zum Entfernen einer Adresse wählen Sie eine Adresse aus und klicken auf **Ausgewählte entfernen**.

Zum Bearbeiten einer Adresse nehmen Sie Ihre Bearbeitung im Bearbeitungsfeld vor und klicken auf **E-Mail aktualisieren**. Beachten Sie, dass sich auch der Benutzername für das Konto ändert, wenn Sie diese Adresse ändern.

Handset-Management

Mit Handset-Management können Sie bestimmte Funktionen für die Geräteüberwachung aktualisieren, den GPS-Aktualisierungszeitrum ändern, die maximale Größe der Protokolldatei steuern und Datenlöschparameter bestimmen. Beachten Sie, dass Aktualisierungen erst empfangen werden, wenn sich das Gerät zum nächsten geplanten Zeitpunkt meldet.

Informativer Hinweis: Handset-Management steht nicht für iOS-Geräte zur Verfügung. Von dem Link für die Einstellungen können Sie Handset-Informationen für das ausgewählte iOS-Gerät, wie z. B. Telefonnummer, Gerätetyp, Gerätename und UDID, anzeigen. (Siehe Abbildung auf Seite 14).

Gehen Sie folgendermaßen vor, um die verfügbaren Einstellungen zu aktualisieren oder zu ändern:

1. Falls nicht schon ausgewählt, wählen Sie aus dem Pulldownmenü **Telefon zum Anzeigen auswählen** oben rechts die Telefonnummer für das Gerät aus, das Sie verwalten möchten.

   Legen Sie in der Spalte **Handset-Management** rechts im Fenster Folgendes fest:
2. Aktivieren Sie das Kontrollkästchen neben **E-Mail-Überwachung**, um diese Funktion für das ausgewählte Gerät zu aktivieren.
3. Aktivieren Sie das Kontrollkästchen neben **SMS-Überwachung**, um die Messaging-Überwachung für das ausgewählte Gerät zu aktivieren.

Copyright © 2012, Juniper Networks, Inc.

4. Aktivieren Sie das Kontrollkästchen neben **MMS-Überwachung**, um die Überwachung von Nachrichten zu aktivieren, die Bilder, Video, Audio- oder andere Multimediaarten für das ausgewählte Gerät enthalten.
5. Aktivieren Sie das Kontrollkästchen neben **Sprachanrufüberwachung**, um diese Funktion für das ausgewählte Gerät zu aktivieren. Die Sprachanrufüberwachung stellt einen Zeitstempel für ein Gespräch bereit.
6. Wählen Sie neben **Grenzwert Protokollereignis** einen Ereignisgrenzwert aus dem Pulldownmenü aus. Wir empfehlen, dass Sie diesen Grenzwert nicht niedriger als 25 einrichten.
7. Wählen Sie neben **Grenzwert Protokollgröße** einen Größengrenzwert aus dem Pulldownmenü aus. Wir empfehlen, dass Sie diesen Grenzwert nicht auf "Off" (Aus) einrichten.

   Der "Grenzwert Protokollereignis" und der "Grenzwert Protokollgröße" arbeiten insofern zusammen, als dass die Einstellung, die zuerst ausgelöst wird, diejenige ist, die wirksam wird. Durch den Ereignisgrenzwert sendet das Gerät eine angegebene Anzahl an Ereignissen (E-Mail, Sprachanrufe, SMS, MMS) jeweils als ein kombiniertes Ereignis, wenn der Ereignisgrenzwert erreicht wird. Dies ist dem Senden jedes einzelnen Ereignisses in Echtzeit vorzuziehen. Wenn das Gerät viele Nachrichten sendet oder empfängt, sollten Sie diesen Grenzwert eher höher einstellen. Ansonsten kann es sein, dass das Gerät kontinuierlich Ereignisse an das Dashboard sendet, was die Leistung des Geräts möglicherweise verringert. Der Grenzwert Protokollgröße schränkt die Menge überwachter Daten, die von dem Gerät gesendet werden, ein. Es wird der zuerst erreichte Grenzwert verwendet.
8. Aktivieren Sie das Kontrollkästchen neben **Bildüberwachung**, um diese Funktion für das ausgewählte Gerät zu aktivieren.
9. Aktivieren Sie das Kontrollkästchen neben **Internetbildüberwachung**, um diese Funktion für das ausgewählte Gerät zu aktivieren.
10. Wählen Sie neben **GPS-Aktualisierungszeitraum** einen Aktualisierungszeitraum aus der Pulldownliste aus. Mit dieser Einstellung können Sie GPS-Aktualisierungen so konfigurieren, dass sie alle fünfzehn Minuten, alle 30 Minuten, stündlich oder täglich vorgenommen werden.
11. Aktivieren Sie das Kontrollkästchen neben **Sperren bei SIM-Änderung**, um diese Funktion zu aktivieren. Wenn diese Funktion aktiviert ist und die SIM-Karte ausgetauscht wird, wechselt das Gerät in den GPS-Diebstahlmodus und wird gesperrt. Sie können das Gerät mit einem Kennwort entsperren.

Informativer Hinweis: "Sperren bei SIM-Änderung" steht nur zur Verfügung, wenn ein Sperrbefehl als Teil des Geräteprofils verfügbar ist.

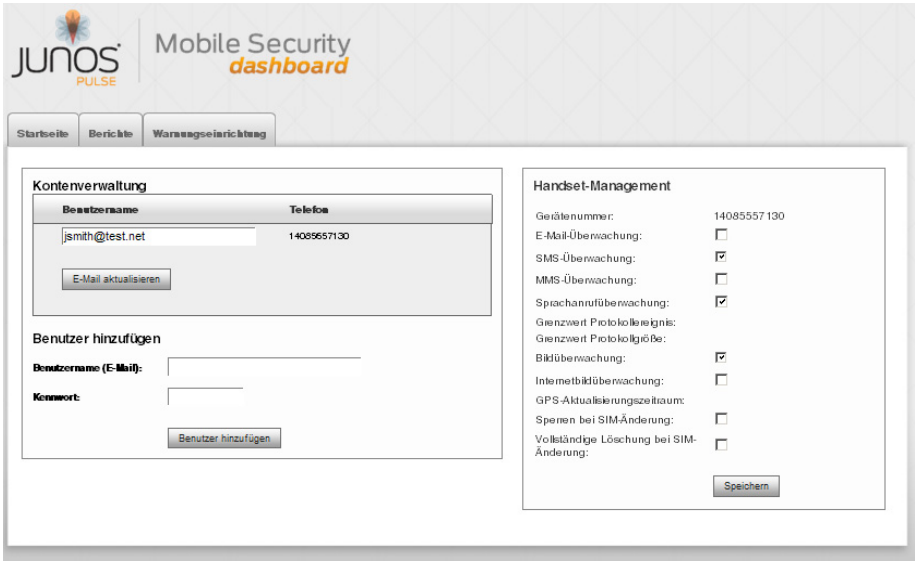
12. Aktivieren Sie das Kontrollkästchen neben **Vollständige Löschung bei SIM-Änderung**, um diese Funktion zu aktivieren. Dieses Kontrollkästchen steht nur zur Verfügung, wenn das Kontrollkästchen "Sperren bei SIM-Änderung" aktiviert ist. Wenn diese Funktion aktiviert ist, werden sensible Geräteinformationen bei einem Austausch der SIM-Karte automatisch vollständig gelöscht.

Informativer Hinweis: "Vollständige Löschung bei SIM-Änderung" steht nur zur Verfügung, wenn ein Befehl zum vollständigen Löschen als Teil des Geräteprofils verfügbar ist.

13. Klicken Sie auf die Schaltfläche **Update** (Aktualisieren), um Ihre Einstellungen anzuwenden.

Copyright © 2012, Juniper Networks, Inc.

Abbildung 10: Fenster "Einstellungen"



Informationen und Konfiguration der Registerkarte "Berichte"

Sie können benutzerdefinierte Berichte mit gesammelten Gerätedaten vergleichen, indem Sie die Kriterien in die in diesem Fenster bereitgestellten Felder eingeben.

Geben Sie zum Ausführen eines benutzerdefinierten Berichts die Berichtskriterien in eines oder mehrere der hier beschriebenen Felder ein.

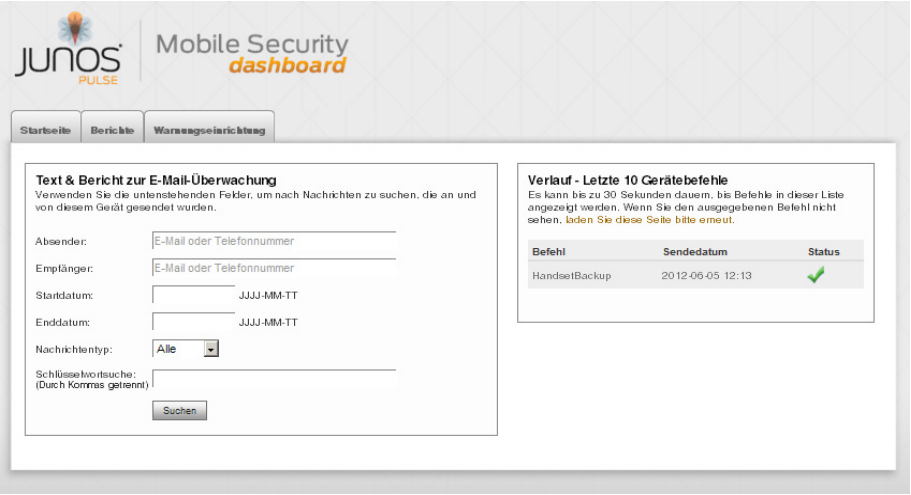
1. Gehen Sie zur Registerkarte **Berichte**. (Siehe Abbildung 11 auf Seite 15).
2. Falls nicht schon ausgewählt, wählen Sie aus dem Pulldownmenü **Telefon zum Anzeigen auswählen** oben rechts die Telefonnummer für das Gerät aus, für das Sie einen Bericht ausführen möchten.
3. Wenn im Bericht Absenderinformationen enthalten sein sollen, geben Sie in das entsprechende Feld die E-Mail-Adresse des **Absenders** oder die Telefonnummer ein. Beachten Sie, dass die Adresse oder die Nummer, die Sie eingeben, mit der Adresse oder der Nummer des Absenders in der Nachrichtenanzeige identisch sein muss.
4. Wenn im Bericht Empfängerinformationen enthalten sein sollen, geben Sie in das entsprechende Feld die E-Mail-Adresse des **Empfängers** oder die Telefonnummer ein. Beachten Sie, dass die Adresse oder die Nummer, die Sie eingeben, mit der Adresse oder der Nummer des Empfängers in der Nachrichtenanzeige identisch sein muss.
5. Geben Sie im Feld **Startdatum** einen Startdatumsparameter für den Bericht ein, den Sie erstellen. Formatieren Sie das Datum mit Jahr-Monat-Tag wie im folgenden Beispiel: 2010-11-24.
6. Geben Sie im Feld **Enddatum** einen Enddatumsparameter für den Bericht ein, den Sie erstellen. Formatieren Sie das Datum mit Jahr-Monat-Tag wie im folgenden Beispiel: 2010-11-24.
7. Wählen Sie aus der Pulldownliste **Nachrichten** den Typ der Nachricht aus, für den Sie diesen Bericht ausführen möchten. Die Optionen lauten: Alle, SMS, MMS, E-Mail, Sprache.
8. Geben Sie im Feld **Schlüsselwortsuche** ein Schlüsselwort oder einen Ausdruck ein, nach dem Sie in den Nachrichten suchen möchten. Nachrichten, die dieses Schlüsselwort enthalten, werden für den Bericht verwendet.
9. Klicken Sie auf die Schaltfläche **Suchen**, um diesen Bericht zu erstellen.

Copyright © 2012, Juniper Networks, Inc.

Verlauf

Auf der rechten Seite des Fensters "Berichte" finden Sie die Spalte **Verlauf**. Hier können Sie die letzten zehn Befehle anzeigen lassen, die an das Gerät gesendet wurden, sowie ihre Sendedaten.

Abbildung 11: Registerkarte "Berichte"



Informationen und Konfiguration der Registerkarte "Warnungseinrichtung"

Durch die Verwendung eindeutiger Bezeichner wie Schlüsselwörter oder Adressen werden Nachrichten, die ein definiertes Kriterium erfüllen, identifiziert und angezeigt**,** indem Sie auf die unter der Registerkarte "Startseite" im Fenster "Startseite" angezeigte Warnmeldung (falls vorhanden) klicken (siehe Abbildung 2 auf Seite 5). Warnmeldungen können auch so konfiguriert werden, dass sie per E-Mail an Sie gesendet werden. Zum Beispiel kann eine SMS-Nachricht, die das zugewiesene Schlüsselwort enthält, automatisch an Sie per E-Mail gesendet werden.

Gehen Sie folgendermaßen vor, um eine Warnmeldung zu konfigurieren:

1. Gehen Sie zur Registerkarte **Warnungseinrichtung**. (Siehe Abbildung 12 auf Seite 16).
2. Falls nicht schon ausgewählt, wählen Sie aus dem Pulldownmenü **Telefon zum Anzeigen auswählen** oben rechts die Telefonnummer für das Gerät aus, für das Sie eine Warnmeldung konfigurieren möchten.
3. Geben Sie in das Feld **Schlüsselwort hinzufügen** ein Schlüsselwort ein, mit dem Sie eine Warnmeldung auslösen möchten, wenn dieses Wort in einer Nachricht, die von dem Gerät gesendet oder auf dem Gerät empfangen wurde, gefunden wurde. Klicken Sie auf die Schaltfläche **Hinzufügen**. Das Schlüsselwort wird jetzt in der Schlüsselwortliste unten angezeigt.
4. Im Feld **Schlüsselwörter** ist auch ein **Kontrollkästchen** vorhanden, mit dem Sie vorgeschlagene Schlüsselwörter aus der Spalte auf der rechten Seite des Fensters verwenden können. Dies sind Schlüsselwörter, die oft als Kürzel in Nachrichten verwendet werden. Um vorgeschlagene Schlüsselwörter anstelle von oder zusätzlich zu Schlüsselwörtern, die Sie eingeben, zu verwenden, aktivieren Sie das Kontrollkästchen **Vorgeschlagene Schlüsselwörter verwenden**. Wenn dieses Kontrollkästchen aktiviert ist, werden die aktivierten vorgeschlagenen Schlüsselwörter als Teil der Warnmeldung verwendet.

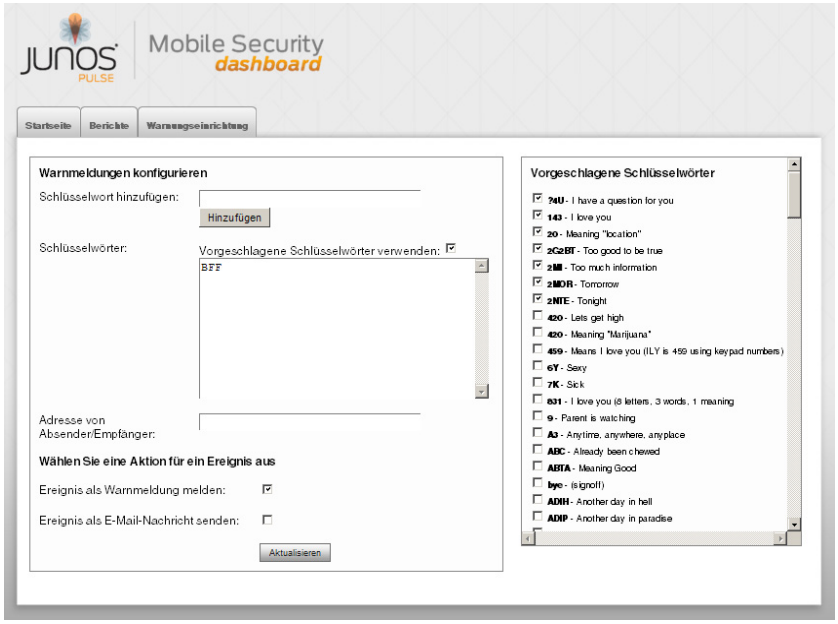
   Sie können durch die Liste der vorgeschlagenen Schlüsselwörter blättern und das entsprechende Kontrollkästchen neben Schlüsselwörtern aktivieren, für die Sie eine Warnmeldung auslösen möchten, wenn sie gefunden werden.

Copyright © 2012, Juniper Networks, Inc.

5. Wenn Sie **Ereignis als E-Mail-Nachricht senden** auswählen, indem Sie das Kontrollkästchen im Feld **Adresse von Absender/Empfänger** aktivieren, geben Sie die E-Mail-Adresse oder die Telefonnummer ein, um nach Warnmeldungen zu suchen. Verwenden Sie diese Funktion, um die Kommunikation mit einem bestimmten Kontakt als Warnmeldung zu markieren.
6. Aus den Optionen **Wählen Sie eine Aktion für ein Ereignis aus** können Sie Folgendes wählen:
   - **Ereignis als Warnmeldung melden**
   - **Ereignis als E-Mail-Nachricht senden**

   Aktivieren Sie eine oder beide Kontrollkästchen.
7. Klicken Sie auf die Schaltfläche **Aktualisieren**, um die Warnmeldung zu aktivieren.

Abbildung 12: Registerkarte "Warnungseinrichtung"


JUNOS PULSE
Mobile Security dashboard
Startseite
Berichte
Warnungseinrichtung
Warnmeldungen konfigurieren
Schlüsselwort hinzufügen:
Hinzufügen
Schlüsselwörter:
Vorgeschlagene Schlüsselwörter verwenden:
BFF
Adresse von Absender/Empfänger:
Wählen Sie eine Aktion für ein Ereignis aus
Ereignis als Warnmeldung melden:
Ereignis als E-Mail-Nachricht senden:
Aktualisieren
Vorgeschlagene Schlüsselwörter
?4U - I have a question for you
143 - I love you
20 - Meaning "location"
2Ge8T - Too good to be true
2M - Too much information
2MOR - Tomorrow
2NTE - Tonight
420 - Lets get high
420 - Meaning "Marijuana"
459 - Means I love you (ILY is 459 using keypad numbers)
6Y - Sexy
7K - Sick
831 - I love you (8 letters, 3 words, 1 meaning
9 - Parent is watching
A3 - Anytime, anywhere, anyplace
ABC - Already been chewed
ABTA - Meaning Good
bye - (signoff)
ADH - Another day in hell
ADP - Another day in paradise

Informationen und Konfiguration der Registerkarte "Support/Hilfe"

Wenn Sie Fragen haben oder technischen Support benötigen, wählen Sie die Registerkarte **Support/Hilfe**. Geben Sie die benötigten Informationen in die verfügbaren Felder ein, und klicken Sie auf **Absenden**.

Informativer Hinweis: Die Registerkarte "Support/Hilfe" ist möglicherweise nicht in Ihrem Dashboard enthalten. Ihr Dienstanbieter kann diese Registerkarte entfernen oder für Ihre Bereitstellung anpassen.

Copyright © 2012, Juniper Networks, Inc.

Kapitel 3

Junos Pulse FAQ

Dieses Kapitel bietet Antworten auf häufig gestellte Fragen.

Junos Pulse FAQs

Ich möchte nicht, dass der Gerätebenutzer die Junos Pulse-Anwendung auf seinem Gerät sieht. Kann ich sie ausblenden?

Wir sind uns bewusst, dass auf manchen Geräten Symbole von der Anzeige ausgeblendet werden können, allerdings kann die Junos Pulse-Anwendung nicht ausgeblendet werden. Zusätzlich zur Steuerung und zur Überwachung stellt Junos Pulse Sicherheitsfunktionen bereit, bei denen der Endbenutzer auf die Konfiguration zugreifen muss.

Was passiert, wenn der Gerätebenutzer die Einstellungen von Junos Pulse auf dem Gerät bearbeitet?

Abhängig von den vorgenommenen Änderungen wird die Änderung ggf. nicht auf dem Mobile Security Dashboard angezeigt. Beispiel: Wenn der Gerätebenutzer Junos Pulse vom Gerät deinstalliert, wird dieses Ereignis nicht im Mobile Security Dashboard angezeigt. Sie bemerken lediglich, dass keine Ereignisse angezeigt werden.

Warum können meine GPS-Koordinaten ungenau sein?

Für diese Ungenauigkeit kann es mehrere Gründe geben. Zunächst müssen Sie bestätigen, dass Sie über ein GPS-fähiges Gerät verfügen und GPS im Datentarif Ihres Netzbetreibers enthalten ist. Wenn die GPS-Funktion nicht in Ihrem Netzwerkdienst enthalten ist, funktioniert sie nicht. Prüfen Sie auch die GPS-Funktion auf dem Gerät, um sicherzustellen, dass es keine Beschränkungen gibt und alle Funktionen aktiviert sind. Kalibrieren Sie Ihren Standort mit dem Gerät über Google Maps von einem Standort mit einem starken Trägersignal. Der beste Standort für den Test ist im Freien. GPS kann auch über Satellit oder das Netzwerk gesammelt werden, mit unterschiedlicher Genauigkeit.

Was bedeutet es, wenn die GPS-Koordinaten 0.0 sind?

Normalerweise kennzeichnet 0.0., dass GPS auf dem Gerät vom Netzbetreiber aktiviert werden muss oder dass diese Funktion vom Netzbetreiber durch Anwendungen von Drittanbietern blockiert wurde. (Beachten Sie, dass wir die GPS-Funktion auf Verizon BlackBerry Curve- und Storm 1-Geräten nicht garantieren können.)

Copyright © 2012, Juniper Networks, Inc.

Wie lange dauert es, bis das Mobile Security Dashboard die Aktivitäten des Gerätebenutzers aktualisiert hat?

Dies kann über das Dashboard konfiguriert werden. Siehe “Handset-Management” auf Seite 12 für Informationen und Richtlinien. (Beachten Sie, dass nicht empfohlen wird, Texte in Echtzeit an das Dashboard zu senden, wenn der Gerätebenutzer große Textmengen sendet und empfängt.)

Kann ich Junos Pulse verwenden, um URLs zu überwachen oder zu blockieren?

Nein, derzeit stellt Junos Pulse diese Funktion nicht bereit.

Wie viele Geräte kann ich mithilfe des Mobile Security Dashboards überwachen?

Die Anzahl der Geräte, die Sie in einem Konto überwachen können, ist nicht eingeschränkt. Um dem Konto ein neues Gerät hinzuzufügen, müssen Sie zuerst die Software auf dem zusätzlichen Gerät herunterladen. Wenn das Gerät mit dem Dashboard registriert ist, können Sie es überwachen.

Ich möchte verschiedene Geräte überwachen, aber jedes Gerät verwendet einen anderen Netzbetreiber.

Der Netzbetreiber spielt keine Rolle. Solange auf dem Gerät ein unterstütztes Betriebssystem ausgeführt wird, können Sie Junos Pulse verwenden.

Copyright © 2012, Juniper Networks, Inc.

Index

A

Aktualisierungsschaltfläche 10, 11
Anti-Diebstahl-Schutz 6
Antivirenaktivität 11
APNS-Zertifikat 10

B

benutzerdefinierte Schaltfläche 12
Benutzername/Kennwortänderung 12
Berichte 14
Bildüberwachung 13

E

Einstellungen 12
E-Mail-Überwachung 12
E-Mail-Validierung 5

F

Funktionen
  Sicherheitsübersicht 2
  Steuerungsübersicht 1

G

Gerät entsperren 7
Gerät sperren 6
Gerät suchen 9
Gerät vollständig löschen 8
Geräteüberwachung 10
GPS
  Aktualisierungszeitraum 13
  Supportinformationen für iOS 10
Grenzwert Protokollereignis 13
Grenzwert Protokollgröße 13

H

Handset-Management 12

I

Internetbildüberwachung 13

K

Kontenverwaltung 12

M

MMS-Überwachung 13
Mobile Security Dashboard
  Übersicht 3

S

Schlüsselwörter, Messaging-Kürzel 15
Scream 9
Sichern Ihrer Daten 11
SMS-Überwachung 12
Sperren bei SIM-Änderung 13
Sprachanrufüberwachung 13

V

Verlauf
  Befehle 15
Vollständige Löschung bei SIM-Änderung 13

W

Warnmeldung 5
Warnungseinrichtung 15

Z

Zurücksetzen des Kennworts 3

Copyright © 2012, Juniper Networks, Inc.

Copyright © 2012, Juniper Networks, Inc.